AUTORITEIT
PERSOONSGEGEVENS

Annual Report 2015

Dutch Data Protection Authority

Preface

Seen from the Dutch Data Protection Authority, the world has slowly changed dramatically, even if we look back only 5 years. We can no longer imagine our daily lives without smartphones, the internet and the development of the Internet of Things. People cannot escape from leaving behind vast quantities of digital personal data traces on a daily basis.

Apps, search engines, social media: they are now usually offered with personal data for payment only. Personal data are thus commercialised. Money as a means of exchange is slowly being replaced by personal data in those areas. But where spending money is one-off and visible, giving out personal data is much less visible and their re-use stays outside everyone's view or control. By using these data – Big Data – we are all profiled. People of flesh and blood become profiles. They are approached and treated based on inimitable mathematical formulas.

Has this made adequate protection of personal data an illusion, a waste of time? Or does compliance with the fundamental right to personal data protection and thus intended personal freedom remain essential for the trust in – and functioning of – society? And if so, what should be done to place personal data protection at the top of the priority list of the public, politics and the press?

The European Data Protection Regulation and the European Directive for the Police and Judicial Authorities derived from it, which are expected to be finalised by the summer of 2016, provide a meaningful beginning of an answer to the latter question. The privacy regulation reconfirms several important principles as they have applied in the European Union since 1995 and contains new elements that may put up a more robust barrier against violation of the right to personal data protection.

For instance, the rights of civilians and consumers will be strengthened and public and private organisations will bear greater responsibility to comply with obligations in the area of privacy. Examples in this context include accountability, privacy by design, and privacy by default. Furthermore there will be an obligation for all public organisations and companies whose relevant activities include personal data collection and processing to appoint Data Protection Officers.

The Data Protection Regulation also sets out a number of more formal issues that will benefit compliance. Contributing factors definitely include a strong position of the regulator, which is equipped with a solid authority to impose penalties, and opening up the possibility for interest groups to take legal action on behalf of civilians so as to have their damages indemnified.

In 2015, as appears from this annual report, the Dutch Data Protection Authority again contributed to compliance with legal provisions on personal data protection. It did so by renewing its website – which

allows civilians and organisations to learn about their rights and obligations faster and more easily – by appearing in the media, parliament and other meetings, by providing legislative advice, but above all by investigations, enforcement and active communication in this regard.

Investigations conducted in the public and private sector have shown that most of the organisations summoned were already willing to bring their procedures in accordance with legal obligations concerning personal data protection as the investigations were conducted. Most of the controllers that were approached often ignored obligations unknowingly or unintentionally. The self-perceived need to act in accordance with the law, however, remains limited.

Apparently, there are insufficient external incentives to prevent violations of the Dutch Data Protection Act. Consumers rarely take action in case of violations because they are unaware in this respect and because violations usually do not result in demonstrable financial losses. In addition, there is little chance of being caught. Dutch government has estimated that over 130,000 organisations in the Netherlands are under supervision of the Dutch Data Protection Authority as they process personal data. In 2015, our budget enabled us to investigate approximately 50 of those. For controllers who are in for a gamble: it looks like the chance of having the regulator knock on your door is less than once every thousand years!

However, since people in our society are increasingly tempted to pay with personal data for various products and services and the re-use of that 'money' is as invisible as it is inimitable, it is inevitable that a number of measures must be taken to organise personal data protection in a more modern way.

One of those measures is a prompt entry into force of new European legislation on privacy. All public and most private organisations collecting and processing personal data will be obliged to hire their own privacy watchdog (the Data Protection Officer). The EU legislation will also result in an increase in certifications of organisations and privacy quality marks being set up. The way in which privacy is safeguarded is an increasing component of marketing strategies. Privacy as a selling point.

A substantial increase in the budget of the Dutch Data Protection Authority is also inevitable. The number of staff at the regulator has been decreasing for years, whereas the number of our personal data that is being processed on a daily basis has in fact increased more than exponentially.

Personal data protection is a fundamental right for good reason. Without this right, the free development and growth of people are at risk. And without an effective protection of this fundamental right, our trust in each other – and eventually in society – is at stake.

Jacob Kohnstamm
Chairman of the Dutch Data Protection Authority

Introduction

In the private as well as the public sector, personal data are the 'new gold'. The working area of the Dutch Data Protection Authority is developing to a great extent, both politically and socially. The Dutch Data Protection Authority supervises compliance with statutory regulations on personal data protection and provides advice on new legislation. Its daily work consists of checking the actual practice against legislation and making considerations at the interface of the fundamental right to personal data protection and innovative services and products.

Every year, the Dutch Data Protection Authority selects a number of themes to focus on in particular. In 2015, themes included profiling, special categories of personal data (sensitive data), local authorities, employment relationships and security. The central theme here was the way in which companies and organisations inform people on how their personal data are processed. People often have no idea of what companies and organisations are exactly doing with their data and what (sometimes far-reaching) consequences this may have. Due to the huge quantities of personal data circulating on virtually everyone and the complexity of processing, it is also very difficult to keep up with. It is therefore essential that companies and organisations are transparent in this respect.

The Dutch Data Protection Authority selects its annual themes based on its knowledge of developments in technology and legislation and based on meetings with stakeholders. Other major sources of information include queries and tips it receives about potential violations, its many press contacts as well as media messages on privacy and data protection.

In 2015, the work performed by the regulator ensured that adequate data protection gained more attention. In addition, most of the companies investigated eventually ceased the identified violations after intervention of the Dutch Data Protection Authority. This usually happened as a consequence of the investigation, but sometimes it was necessary to warn with sanctions.

Below, you will find a selection from the work performed by the Dutch Data Protection Authority in 2015.

Profiling

Profiling means categorising individuals based on patterns and (accidental) correlations within databases. Its major risks include a lack of transparency on information collection and the possibility of making wrong decisions, e.g. at border controls and in social security. Investigations conducted in the sectors of the internet and telecom on which the Dutch Data Protection Authority published in 2015 have also shown how versatile and widespread profiling is. Websites, social media, search engines, apps, smart TVs – the use of profiling is more of a rule than an exception. This means that people are approached based on profiles.

In its investigations, the Dutch Data Protection Authority underlined the legal requirement of informing people in advance on processing their personal data. In response to the investigations conducted by the regulator, Nederlandse Publieke Omroep (Dutch Public Broadcaster), Ziggo (Dutch provider of cable TV) and TP Vision (manufacturer of Philips smart TVs), *inter alia*, have now improved their information to users. And the Dutch Data Protection Authority imposing an order on Google subject to a penalty payment in case of non-compliance has resulted in a tightened privacy policy and a public campaign.

Sensitive data

Data on someone's religion, race, political opinions, health and previous convictions fall within the category of sensitive data. Since this is sensitive personal information, these data can only be collected, stored and used under strict conditions. In 2015, medical and criminal data received special attention from the Dutch Data Protection Authority. It selected this focus because an increasing number of people use apps and devices to monitor their health and lifestyle – with all its consequences for the processing and protection of health data. In addition, the regulator identified an increase in public private partnerships in the security domain, leading to new data exchanges between government organisations, companies and civilians.

An investigation conducted by the Dutch Data Protection Authority in 2015 showed, *inter alia*, that lifestyle apps may collect and analyse health data – often without users being aware of it. The regulator pointed out to software providers that additional privacy-protecting measures are required in this context, including clear information to users.

In the context of criminal data, e.g. in police files, the importance of proportionality and subsidiarity tests were emphasised by the Dutch Data Protection Authority in 2015. This was the Authority's response to a Foresight Study on the Dutch Data Exchange Framework Act, with which Dutch government intends to solve several problem areas in tackling fraud at partnerships. The broad base for data exchange, however, is at odds with the legal requirements of proportionality and subsidiarity, said the Authority.

Personal data at local authorities

Since several tasks were transferred from central government and provinces to municipalities, local authorities have had new responsibilities in the areas of youth care, social support, employment and care for the chronically ill and disabled. In 2015, the Dutch Data Protection Authority drew attention to the privacy risks of decentralisations in the social domain in various ways.

First of all, the Dutch Data Protection Authority published the outcome of website quick scans of approximately 50 municipalities in 2015. It turned out that on many websites it was difficult to find information on data processing within the social domain. One of the questions the regulator asked in the investigation following the quick scans was to what extent municipalities are transparent when it comes to processing their residents' personal data.

The Dutch Data Protection Authority also assessed data processing in youth care. The regulator published the outcomes of investigations it had conducted at two Youth Care Agencies where the registration of personal data of clients was not going well. In addition, the Authority provided advice on the duty of confidentiality as per the Dutch Youth Act. According to the regulator, a lawful breach of confidentiality to provide personal data has not been set out properly in what is referred to as the 2015 VWS Catch-all Act (VWS: Dutch Ministry of Public Health, Welfare and Sport). On the insistence of the Dutch Data Protection Authority, several strict conditions were attached to the Youth Act Provisional Scheme for Personal Data on Invoices, which anticipates a formal amendment to the Youth Act.

Personal data in employment relationships

Cameras monitoring shop personnel. Employers collecting data on sick employees. Employment agencies doing background checks on jobseekers. In practice, privacy and data protection do not come naturally for employees and jobseekers. In 2015, the Dutch Data Protection Authority drew attention to, *inter alia*, the protection of medical data in sickness absence registration systems and the protection of Suwinet.

In 2015, the Dutch Data Protection Authority sent letters to dozens of administrators of sickness absence registration systems to point out their responsibilities concerning the protection of software and applications. An earlier investigation of Humannet sickness absence registration systems had shown that protection was insufficient.

In 2015, as in 2014, the Dutch Data Protection Authority investigated the protection of Suwinet, a system which is used by, *inter alia*, municipalities, UWV (Employee Insurance Agency) and the Social Insurance Bank to exchange personal data in the areas of work and income. Building on the investigation into UWV and the municipality of 's-Hertogenbosch, the Authority started investigating the method of operation at other municipalities in 2015.

Protection of personal data

The personal data of an average Dutch person may be stored in hundreds or even thousands of databases of companies or government organisations. These data must be adequately protected by law. This is to prevent e.g. data breaches and abuse such as identity fraud. In 2015, as in previous years, the Dutch Data Protection Authority conducted an investigation into violations of the legal requirement of adequately protecting personal data.

In this context, the Dutch Data Protection Authority pointed out in October 2015 that, with the current state of the security situation, it cannot be ruled out that unauthorised persons find out DigiD login data of users. This would enable unauthorised persons to abuse sensitive data which are accessible with DigiD. The Dutch Data Protection Authority therefore called for an additional security device at government organisations which are connected to DigiD. At the same time, the Authority published the outcome of its investigation at advertising agency Digi-D, which got hold of login data of 8,500 DigiD users. The advertising agency took measures following the investigation.

Across the border

In a globalised society, international cooperation between privacy regulators is more important than ever. Because the internet does not have borders, for example. The Dutch Data Protection Authority therefore works in close cooperation with counterpart regulators in Europe and beyond. The Dutch Data Protection Authority is a very active participant in European partnerships, including the Article 29 Working Party, the Berlin Telecom Group and the supervisory bodies for, *inter alia*, Europol and Eurojust. In 2015, the Authority signed two cooperation agreements.

Within these international cooperative arrangements the Dutch Data Protection Authority was also involved in processing medical data in health apps, transferring personal data to the United States, and the European Passenger Name Record system, which stores personal travel information from computer reservation systems. As in 2014, the regulator spent much time on revising European privacy legislation. One of the highlights of the international activities of the Dutch Data Protection Authority was the International Data Protection and Privacy Commissioners Conference, which was held in Amsterdam in October 2015. With more than seven hundred participants from all over the world, the conference served as a multi-disciplinary platform to share experiences, share knowledge and make plans together. During the conference, the final outcome of the Privacy Bridges Project was presented, with ten proposals to bridge trans-Atlantic differences concerning data protection.

New power and new task

Until 1 January 2016, the Dutch privacy regulator had very limited powers to impose penalties if the Dutch Data Protection Act was violated. It could only impose an order subject to a penalty for non-compliance and violators were first given a period of time in which they could cease violations. Since 1 January 2016,

the authority to impose penalties has expanded significantly. The Dutch Data Protection Authority can now also impose penalties if personal data are processed negligently, stored longer than necessary, or protected insufficiently by government organisations or companies. The new authority to impose penalties is expected to encourage compliance with the law due to its preventive effect.

In addition, the data breach notification obligation took effect on 1 January 2016. This obligation means that organisations (companies as well as governments) must immediately notify the Dutch Data Protection Authority as soon as they experience a serious data breach.

In 2015, the regulator published policy rules which can help organisations determine whether a data breach is in order and if so, whether they must report this breach to the Dutch Data Protection Authority and possibly to the data subjects.

"Protecting personal data is expected to receive much more priority when developing products and services. The data breach notification obligation is not an end in itself, but a means to ensure data breaches are prevented."
Jacob Kohnstamm, Chairman of the Dutch Data Protection Authority

Working method
The Dutch Data Protection Authority supervises processing of personal data in order to ensure compliance with laws that regulate the use of personal data. The most important laws are the Dutch Data Protection Act (Wet bescherming persoonsgegevens), and the Police Data Act (Wet politiegegevens). In order to encourage compliance, the Authority uses a mix of instruments in the areas of supervision, enforcement and communication.

Supervision
The Dutch Data Protection Authority must make choices when investigating alleged violations of the law. It uses several criteria to determine whether an investigation will be conducted. The Authority will conduct an investigation when there is a suspicion of serious and structural violations that affect many people, the regulator can make a difference based on its powers, and the violations fall within the themes set by the regulator annually.

In addition to conducting investigations, the Dutch Data Protection Authority can also act by sending warning letters and entering into discussions. This is done predominantly in cases where the above criteria are not met. These letters or discussions usually suffice to cease a violation. If required, the regulator can still conduct an investigation if the violation continues or starts again after some time.

Enforcement
The Dutch Data Protection Authority may take enforcement action if it identifies violations that continue persistently after the investigation. The Authority has the power to impose an order subject to a penalty for non-compliance. In these cases, violators of the law will be given a certain period of time to adjust their working method. If they fail to do so, they will have to pay a penalty. Since 1 January 2016, the regulator also has the power to impose a penalty.

Communication
Communication – combined with monitoring and enforcement – is a major instrument to encourage compliance with the law. The Dutch Data Protection Authority therefore maintains close contact with the media. In addition, discussions are held with trade organisations and other stakeholders and lectures, presentations and other events are regularly given by members of the Authority, members of the

management team and staff members. In addition, the Authority provides information by way of telephone consultation hours and it offers comprehensive information and guidance through its website autoriteitpersoonsgegevens.nl.

Annual report

The annual report provides an overview of the core activities of the Dutch Data Protection Authority. This edition, reporting on 2015, contains an appendix with numerical data, which can be found online via autoriteitpersoonsgegevens.nl/15/2. The '2015 in a nutshell' summary is available via autoriteitpersoonsgegevens.nl/15/3.